Enterprise Security and Risk Management Office

Monthly Cyber Security Tips

NEWSLETTER

MAY 2007 Volume 2, Issue 5

Unintended Information Disclosure

From the Desk of Ann Garrett, Chief Information Security Officer

Organizations rely on information for all of their core business functions. They collect, process, store and transmit all kinds of citizen and customer information, and sometimes that information is confidential or sensitive in some way.

The March 2007 Cyber Security Tip on "Safeguarding Your Data" discussed several methods you can use to define and protect the information your organization uses and for which it is responsible. But what happens when those protection mechanisms fail? What happens when the information you are protecting is unintentionally disclosed? This month's Tip will help you understand what unintended disclosure means and how serious the issue is. It will also outline how your organization's protected information can become exposed, how you can respond to such an incident, and how you can help prevent such incidents from occurring.

Unintended Information Disclosure

"Unintended" disclosure is the malicious or accidental disclosure of confidential or sensitive information. Often this entails exposure to individuals outside your organization, but it can also mean exposure to unauthorized individuals inside your organization. The kinds of information at risk can be confidential data such as financial accounts, credit cards, Social Security numbers, personal medical information, or other personally identifiable information defined by law or by your organization's data classification policy. Other vital information at risk can include secret, top secret, or other federal, state, or organizationally protected information.

Many of the items we see in the news about security breaches involve information that can be used for identity theft. Depending on what kind of data is exposed, it can also lead to other criminal activity like extortion, or it can be used for an attack on critical infrastructure systems operated by the government, finance, transportation, utility, chemical and telecommunication sectors.

How serious is the issue?

Unintended information disclosures occur though a variety of means. Electronically, they can result from lost backup tapes, lost thumb drives, lost laptops, exposure via website attacks, email exchanges, or from other electronic communications or data storage exposure. Disclosure can also occur from non-electronic means - discovering paper files in trash bins, overhearing phone conversations and shoulder surfing are all examples of this.

Several organizations have been tracking data breaches to help determine risks and trends. One of the types of data at risk is Personally Identifiable Information (PII). Privacy Rights Clearing House started tracking incidents involving PII after the Choice Point data breach on February 15,

2005. Between January 1, 2005 and April 30, 2007 over **153,000,000** records have been exposed to potential identity theft in known reported breaches. This does not include records exposed in unreported breaches.

Many of the more notable reported PII breaches have occurred in large businesses or in federal agencies. However, state and local governments, local businesses and small organizations have also suffered information disclosure incidents. Many other breaches involving information such as confidential customer lists, proprietary source code, passwords or network maps occur with alarming regularity, but are not always tracked or even reported. No organization is immune.

These incidents represent significant financial costs. Costs will be incurred from incident investigation, the technical response of fixing the problems, informing affected persons, credit checks and loss from financial theft; all of which can vary. The total cost of a breach could range from thousands to millions of dollars.

Just as importantly, such an incident can result in the loss of public confidence in the organization and its leaders, or if the information disclosed relates to physical or personal safety, the it can aid in attacks on people or critical infrastructures and can even result in the loss of life.

How can I respond to an information disclosure incident?

- First and foremost, realize that we are all responsible for information security – reporting the incident is the right thing to do. Not only are you helping to limit the damage the breach may create, you may be able to help stop it from happening again.
- Be aware that disclosure laws vary from state to state and policies will vary from organization to organization. You may be required to report information disclosure incidents. Review your organizations policies and response procedures for the most appropriate actions to take.
- If you are unsure what those policies and procedures are, or if they do not exist, report the incident to your supervisor. Document what you know – what happened, when it happened, where it happened, so your management and your incident response team have the most accurate information possible.
- If you think your personal financial information has been compromised, contact the data holder to confirm the incident, and contact your financial institution or credit company to initiate protection mechanisms for your accounts. The Federal Trade Commission also has excellent guides to both preventing and responding to identity theft.

How can I help prevent unintended information disclosure?

- Know what kind of data you are handling or the data your system is storing and processing, whether electronically or on paper.
- Classify your organization's data and protect it according to its value and risk.
- Follow your organization's security policies and procedures. These will help you protect against both malicious and accidental information disclosure.
- Follow the least privilege and role based rules for allowing access. Limit access to confidential information to only those people or roles that require access.
- Know your organizations data retention policies – don't store confidential information longer than necessary.
- Use privacy statements in electronic and paper documents.
- Don't use confidential data for testing systems or applications.
- Store, transport, and destroy confidential data responsibly. Protect data with encryption and access controls when appropriate, and adequately erase or destroy electronic storage devices. Don't take confidential information home or when traveling unless

authorized. When disposing confidential documents, use a shredder.

- Keep portable data storage devices like laptops, CDs, blackberries, flash drives, and backup tapes in secured locations – it only takes a few seconds to steal these valuable items.
- Remember that cyber security is everyone's responsibility and that you can make a difference.

For more information:

MS-ISAC Safeguarding Your Data
http://www.msisac.org/awareness/news/2007-03.cfm

MS-ISAC Erasing Information and Disposal of Media
http://www.msisac.org/awareness/news/2006-08.cfm

Privacy Rights Clearinghouse
http://www.privacyrights.org/

FTC – Identity Theft
http://www.ftc.gov/bcp/edu/microsites/idtheft/

Federal Identity Theft Task Strategic Plan
http://www.idtheft.gov/reports/StrategicPlan.pdf

Sample Data Classification Matrix for Governments
http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html

Sample Data Classification Strategy
http://www.yourwindow.to/information-security/gl_dataclassification.htm

Data Classification Sample Policy
http://my.gwu.edu/files/policies/DataClassificationPolicy.pdf

California Office of Privacy Protection Recommendations
http://privacyprotection.ca.gov/recommendations/recomend.htm

Brought to you by:

MS-ISAC

http://www.msisac.org